B. Duty to Warn

The Commission suggests that it might be appropriate to require a change in LECs' tariffs (i.e., those limiting liability for fraud) to incorporate a "duty to warn" in certain circumstances.[73] As the Commission states, "[i]f customers are unaware of potential liability, they are unlikely to take steps to limit their exposure."[74]

U S WEST does not believe that such a tariff amendment is necessary, although we would not see one as per se objectionable. We do warn our customers about the latent risks associated with the various products we sell -- ranging from network services to calling cards to CPE. And, we advise them of their financial responsibility in those cases where fraud occurs.[75] We believe that other LECs and carriers do the same. Therefore, we are not certain that the amendment of tariffs to include such a duty will be substantially meaningful.

C. Absolute Caps on Customer Liability

The suggestion of one of the recent toll fraud complainants was that it was unreasonable for a carrier to demand collection for toll fraud committed via a PBX, in light of the fact that had

[73] See NPRM ¶ 24 ("[W]e tentatively conclude that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks of using carrier services are unreasonable.").

[74] Id.

[75] See Appendix B at 2.

the toll fraud been committed via a calling card, the customer's liability would have been limited to $50.[76] At an unreflected level, the variances in results might appear unfair. But the policy determinations associated with each have been set by different agencies with different histories.[77]

As mentioned above, traditionally, a customer has been considered responsible for all common carriage traffic traversing the network from that customer's station. And, prior to the determination by Congress and the Federal Trade Commission ("FTC") that telephone calling cards should be treated like traditional credit cards for purposes of issuance (that they cannot be issued unsolicited) and limitation of liability purposes,[78] callers were responsible for all fraud charged to their calling cards.

The wisdom of that decision is not here open for discussion or debate. But the end result is clear: a consumer can be much less concerned about fraud resulting from a calling card than

[76] See Chartways Technologies, Inc. v. AT&T Communications, Memorandum Opinion and Order, 8 FCC Rcd. 5601-02 ¶ 4 (1993).

[77] See NPRM ¶ 38.

[78] See 15 USC § 1643; 12 CFR § 226.12(b)(1).

from his/her station, because -- above and beyond the $50 limit -- the customer has no financial liability.[79] Clearly, that fact affects customer's behavior.

While most customers, undoubtedly, do not openly trade in their calling card numbers, any trip to an airport will demonstrate that they also do not cup one hand over their dialing fingers to protect against "shadowing." *If* consumers were subject to greater liability for calling card fraud, they undoubtedly would take more care in using them.[80]

Caps on end-user liability for fraud create disincentives to managing the problem of fraud[81] -- even when made possible or

[79] The difference between the end user's liability for calling card fraud and the fraud actually resulting is one reason carriers have an independent motivation to design and implement networks that are secure against fraud. *Compare NPRM* ¶¶ 25, 38. As more and more customers take advantage of "on-the-move services," more and more telecommunications traffic will be billed to cards.

This is *not* to say, however, that if an end user were held absolutely liable for all fraudulent calling on a calling card that network providers would lack an incentive to protect against fraud in their networks. When customers cannot pay bills, whether because the bill got too high through voluntary activity or through fraud, customers do not pay -- there is an uncollectible. The press of the uncollectibles produce an independent motivational force for carrier fraud prevention capabilities in the network.

[80] While the Commission may be correct that "cardholders are under an affirmative obligation to report lost or stolen credit cards immediately, and to protect against theft of their card numbers," (*id.* ¶ 38) the fact that there is no consequence for failure to do what is obliged (beyond the $50 liability) predictably undercuts the urgency of the obligation itself.

[81] *Compare id.* ¶ 21.

contributed to by the customer's own behavior. Thus, U S WEST encourages the Commission to reject such concepts.

D. The Need to Mandate Carrier Fraud Prevention Services

The Commission inquires as to whether it should "require IXCs and LECs to offer customers protection through monitoring services, on what basis those services should be offered, and whether such services should be part of the basic interexchange service offering."[82] The only rationale for requiring carriers to offer such products would be that the Commission was assigning certain fraud-prevention responsibilities to the carrier (as part of its common carriage responsibility), because it considered the responsibility for fraud prevention to be appropriately lodged there.[83] U S WEST disagrees with such position.[84]

[82] Id. ¶ 26. The Commission does not specifically define "monitoring services," but U S WEST takes this to mean services that monitor/track toll usage and alert (someone) when the usage appears out of line. Compare id. ¶¶ 16-18 (where commentors allege that carriers are in the best position to monitor customer traffic for fraud).

[83] The Commission's suggestion could be considered as another "if they bear the loss, they will work harder on prevention" proposal, i.e., if carriers had to bear the loss, they would create network monitoring services to protect themselves (as well as their customers) against such losses.

[84] In arguing against this suggestion, U S WEST should not be interpreted as saying that we do not believe that monitoring services should be created in the network because, after all, we do not bear the risk of the completed fraudulent transaction. Rather, we have some fundamental jurisdictional considerations about the Commission mandating such services, as well as some evidence to suggest that the market would not be willing to pay for them.

As a basic philosophical matter, U S WEST does not believe that the Commission should be in the position of ordering carriers to provide services.[85] Such decisions are most appropriately left to the carriers themselves, made after assessing the needs of their customers.[86]

But, in addition to our philosophical position, U S WEST sees no demonstrated need for the Commission to act in this matter. As we stated earlier, U S WEST has minimal intraLATA fraud.[87] Thus, clearly, as a LEC we should not be compelled to expend funds to protect against fraud primarily occurring in the interLATA, interstate arena.

Additionally, there are monitoring products currently available to customers, albeit for a price.[88] U S WEST sees nothing untoward about carriers charging customers for fraud prevention controls. Not all customers need such protection, and we see no reason to build in the costs of all "fraud protection" to either the basic local exchange or interexchange service offerings, as the Commission suggests.

Certainly, as is clear from the above text, some fraud prevention activity is already included in the price of basic

[85] And, as a matter of jurisdiction, the Commission is not in a position to do such a thing, in any event, absent a Section 214 hearing. See 47 USC § 214.

[86] See American Telephone and Telegraph Company v. FCC, 487 F.2d 865 (2d Cir. 1973).

[87] See supra note 14.

[88] See NPRM ¶¶ 25-26 (citing to MCI Detect, AT&T NetProtect and SprintGuard).

network service offerings. A carrier has an independent motivation to control fraudulent telecommunications traffic, even if a customer has no interest in purchasing a product to do so. But a carrier should not be compelled to create usage and traffic monitoring systems in its network in the absence of a demonstrated need, demand, and an ability to recover its investment. That assurance is not obvious in the existing market configuration.

U S WEST has looked at certain traffic monitoring network equipment. It is extremely expensive. While a decade ago there may have been some relevance in a discussion about where fraud network monitoring should be done, over the last ten years IXCs have invested heavily in their own networks to create fraud prevention controls. Thus, U S WEST has reason to believe that IXCs/OSPs would not be willing to pay the price necessary to warrant LEC network fraud monitoring investments. And, given that network fraud protections already exist with regard to interLATA, interstate networks, LECs should not be compelled to create duplicate or redundant capabilities.

V. CONCLUSION

Telecommunications fraud is a serious problem. But, it is not a problem being ignored or taken casually. Telecommunications providers, CPE manufacturers, entrepreneurs, industry associations and law enforcement personnel are all working together to devise better fraud prevention mechanisms.

The work of these entities should be applauded, not duplicated. Thus, the Commission's focus should be on whether there is anything it can do by rulemaking that can enhance the fraud prevention activities already in existence. U S WEST does not believe that there is.

With regard to LECs in particular, U S WEST is confident that filed comments will resemble our own in detailing the already extensive work being done to prevent and control fraud, ranging from customer education to the development of network access and screening mechanisms. We are confident that the evidence submitted will debunk any theory that LECs are not sufficiently pro-active in the area of fraud prevention because they enjoy a limited liability with respect to fraud liability.

The Commission should not manipulate carriers' existing tariff limitations of liability with respect to fraud liability, for at least two reasons. First, limitations of liability are of broad application and should not be required to be changed for a particular class of customer with a particular kind of problem. Second, carriers' existing limitations of liability currently operate with regard to fraud in a manner properly aligned with sound risk management principles, both with regard to prevention and loss liability. The entity that either controls or has responsibility for the CPE originating or terminating a telecommunications transaction should be the responsibility (and attendant costs) associated with that access. While LECs can aid customers in controlling such access, they cannot make choices for them, or guarantee against human conduct or behavior, especially conduct criminal in nature.

For the above reasons, U S WEST submits that the Commission need not proceed further with this proceeding, other than to encourage current fraud prevention efforts to remain robust. It might also wish to set up some kind of internal bureaucratic mechanism so that it receives minutes of industry association meetings, or the like, in order to remain well informed of the ongoing fraud prevention activities.

Like many other telecommunications issues, U S WEST believes that the marketplace and the industrious conduct of the players in that marketplace will provide resolution of certain fraud problems. It will not eliminate them, to be sure. The world of electronics, computers and digital communications brings with it its own inherent intrigue to those interested in free carriage. Those interested in carriage for a fee will remain motivated to design and deploy networks capable of rendering to them amounts properly due and owing. There is probably no regulatory motivator more forceful than that.

For the above reasons, U S WEST would encourage the Commission to reflect seriously on whether or not the current docket needs to be extended beyond the instant pleading phase (i.e., comments and replies). If it is demonstrated that nothing materially helpful can be done by allowing the proceeding to remain open and that no rules need to be promulgated, U S WEST would encourage the Commission to terminate the proceeding.

Respectfully submitted,

U S WEST COMMUNICATIONS, INC.

By: Kathryn Marie Krause /lc

Kathryn Marie Krause
Suite 700
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Its Attorney

Of Counsel,
Laurie J. Bennett

January 14, 1994

ATTACHMENT A

November 15, 1993 US West Today.

CUSTOMER FOCUS

MCI toll fraud expert praises BGS program

PHOENIX — A toll fraud prevention program from U S WEST Communications Business & Government Services was the focus of discussion during a recent National Toll Fraud Prevention Committee meeting here.

One of the national group's agenda items was to request local exchange companies institute education programs for large business and government segments — similar to what BGS already does.

Dave Jordan, an industry liaison on toll fraud for MCI, praised the toll fraud prevention program the U S WEST market unit offers clients and employees.

Jordan told the gathering, "U S WEST has the vision to address the issue and has a flourishing program for business customer education. Now we've got to get other Bell Operating Companies on board."

The national group is composed of local exchange companies, including representatives from Bell Operating Companies, interexchange carriers and other telecommunications providers. Toll fraud costs the industry $3 to $5 billion a year in lost revenue.

"Interexchange carriers are limited in what we can do alone," he adds. "We don't have as direct an access to customers as do local exchange companies."

BGS, which began a toll fraud prevention program a year ago, will next month wrap up a series of eight seminars, featuring toll fraud experts inside and outside the industry, for employees and customers in major metropolitan areas.

Pleased customer *— MCI toll fraud expert Dave Jordan touted the U S WEST Communications Business & Government Services' toll fraud prevention program at a national meeting. He holds a booklet BGS published for employees and customers.*

ATTACHMENT B

Vital Information
For Your
Organization

Toll fraud is big time crime.

US WEST
COMMUNICATIONS

Making the most of your time

Table of contents

Who *are* these people?	page 2
PBX fraud	page 4
Safeguards and countermeasures	page 5
Voice mail fraud	page 6
Safeguards and countermeasures	page 7
Cellular fraud	page 8
Safeguards and countermeasures	page 9
Hacking	page 10
Safeguards and countermeasures	page 11

Toll fraud: A common sense approach to minimizing your risk

Toll fraud — the theft or misuse of communications services — costs American business and government billions of dollars annually.

Virtually every communications system — be it Private Branch Exchange (PBX), voice mail, cellular or central office based — is vulnerable to toll abusers.

Crooks looking to penetrate your communications system operate in a variety of ways. They steal authorization numbers, crack access codes with computer programs, employ illegally altered cellular telephones — even take control of voice mailboxes.

How real is the threat? Consider these documented cases:

■ One firm discovered — too late — that thieves had accessed its PBX system to place more than 30,000 international calls with a total value of $430,000.

■ A group of toll abusers whose efforts had been detected sought a unique form of revenge. They pried their way back into the user's system, and — for 45 minutes — dialed 911 to report numerous fake accidents and disasters.

Continued on next page

■ In a stunning display of bravado, computer crooks targeted an office of the U S Drug Enforcement Administration, making $2 million worth of domestic and international calls over an 18-month period.

■ $50,000 was the tab for fraudulent calls placed through an unsuspecting user's voice mail system. The organization had made the mistake of choosing simple, two-digit access codes.

Who pays? The law has clearly established that the toll fraud victim is responsible for all charges. Because equipment controlled by the user makes fraudulent calls possible, local telephone companies and interexchange carriers will not assume responsibility for losses due to toll fraud.

You needn't be a large user in a major city to become a target. Toll fraud schemes that originate in New York, for example, use communications systems located virtually anywhere in the U.S. Small to moderate sized organizations face special risks because many lack the expertise to identify and deal with toll fraud quickly and effectively.

We at U S WEST Communications are committed to fighting toll fraud. Our objective is to make you aware of the problem, and to suggest ways in which you may minimize your risk.

Toll abusers are both inventive and tireless. Known in their shadowy world as hackers, crackers or phreakers, they invade computer and telecommunications systems for fun and profit. Toll criminals tend to fall into one of the following categories.

The professional thief

■ These individuals seek to use your toll circuits, cellular telephones or voice mail service for profit. They steal access codes, calling cards and credit card numbers — or crack access codes with computer programs known as "war dialers."

Your access numbers may be used by the original hacker or may be peddled on street corners, on college campuses, through informal hacker networks or via pirated voice mailboxes.

Recent refinements in toll thievery include highly organized call-sell operations. Some use pay telephones. Others employ "phone rooms" or "phone houses" equipped with numerous cubicles and telephone sets. Customers pay the seller's price and tell an "operator" what number to dial. The call is then connected and is billed to a stolen access code.

The drug dealer

■ Tipoffs to drug dealing through your communications system may include cryptic messages in your voice mailboxes, foreign-sounding conversations, and uncharacteristic telephone traffic to such countries as Colombia, Bolivia, Mexico, the Dominican Republic and Pakistan.

Drug dealers normally are not concerned with cost, but they do require secrecy — a valuable commodity available through stolen authorization codes. Drug dealers' calls may originate almost anywhere, but they can be traced only to the PBX or voice mail system that authorized them and routed them over the public switched network.

The corporate snoop

■ Increasingly these days, industrial espionage involves gaining access to competitors' voice mail systems. Once inside, intruders can check mailboxes for proprietary information, erase or alter important messages and spread disinformation with their own bogus messages.

As an employee, you're the first line of defense against snoops and hackers. Keep codes and access numbers to yourself

It's regrettable but true that threats also may come from within. Voice mailboxes can be easy prey for unscrupulous employees who, for whatever reason, wish to pry into the affairs of their colleagues or superiors.

The disgruntled former employee

■ Revenge is usually the motive here, and the consequences can range from annoying to catastrophic.

The disgruntled former employee may possess knowledge that can be a significant threat. These individuals have been known to change or delete important voice mail messages, to leave threatening or harassing messages and to sell passwords and access codes for cash. Even more sophisticated and damaging forms of vandalism should be considered a possibility.

The recreational hacker

■ To certain high-tech types, attacking a computer or telephone system is like a real-life video game; it's a challenge to be met and mastered. They seek "bragging rights" from their peers. These individuals — most of whom are high school or college-age computer whizzes — often enjoy hacking around in a PBX or voice mail system just to see how much chaos they can create. They commonly trade stolen access codes and passwords like baseball cards. The recreational hacker's intent may or may not be malicious. In either case, however, the results are anything but entertaining for the victim.

PBX Fraud

The most common forms of toll fraud exploit the remote access capability built into on-premise switching hardware.

Remote access is a convenient, cost-saving feature for PBX owners. It allows their employees to dial into the system via 800 number or other special access number. Once inside, the caller receives dial tone from the PBX and, in response, enters a numeric authorization code. If the PBX recognizes the code, it allows for placement of a long distance call that is billed back to the PBX owner. Unfortunately, remote access is also a convenient, cost-saving feature for toll abusers. Unauthorized persons who gain access to a PBX can place long distance calls — or even sell long distance services to others — while the toll costs accrue to the PBX owner.

Toll abusers invade PBX systems in a variety of ways. They snoop around offices, eavesdrop in airports and rummage through dumpsters in search of access codes. Many employ computer programs that search for PBX units and run random numbers until they achieve a "hit" that cracks a code and opens the gateway to the public switched network.

Symptoms of PBX-based toll fraud include:

- sequential dialing of incoming calls
- a high volume of unusually short or long calls
- unexplained increases in incoming or outgoing calls
- frequent hangup, crank or obscene calls
- interception of foreign language conversations
- calls terminating in foreign countries
- sudden increases in 800 usage
- changes in after-hours calling patterns
- system blockage, with employees unable to call in or out because circuits are busy

While some organizations detect these invasions quickly, others may remain unaware of toll thievery for weeks — or even months. Massive long distance charges can result.

Some experts estimate that a skilled hacker equipped with a code-generating program can crack a three- or four-digit code in five minutes, a six-digit code in a matter of hours.

PBX-based toll fraud—safeguards and countermeasures

- Be alert to the symptoms of PBX abuse.

- Delete all authorization codes programmed into your PBX for purposes of testing and service.

- Consider eliminating remote access to your PBX and replacing it with telephone credit cards for appropriate personnel.

- If you eliminate remote access, have your vendor remove or disable this feature. If your PBX remains access-ready — with unprotected modems — hackers can enter the system and activate remote access for themselves.

- Investigate any toll fraud monitoring options that may be available from your interexchange carrier.

- Consider purchasing a Direct Inward System Access security device. Contact your hardware vendor for details.

- Assign security codes only on a need-to-know basis. Each employee should have his or her own code. No sharing.

- Do not allow employees to create their own codes. Assign code numbers on a random basis, using the maximum number of digits possible. Although lengthy codes are undeniably inconvenient, they are — regrettably — becoming a necessity for organizations intent on discouraging toll fraud.

- Do not associate codes with employees' telephone extension numbers, employee i.d. numbers, social security numbers, birthdays, anniversaries, addresses and other common numerical sequences. It's surprisingly easy for hackers to break such codes.

- Implement a barrier code system. A barrier code is an additional numeric password that adds a second level of security.

- Change access and barrier codes periodically. Do not use voice mail messages to notify employees of code changes.

- Deactivate all unassigned access codes. Codes of employees who leave your organization should be deactivated immediately.

- Do not allow unlimited attempts to enter your system. Have your PBX programmed to disallow access after the third invalid barrier code or access code attempt.

- If practical for your organization, restrict remote PBX access to normal business hours.

- Assign employees restriction levels based on their needs. Chances are, for example, that few employees require access to international long distance service.

Continued on next page

■ If you use 800 service, purchase only the geographic coverage you really need. Purchase 800 service call detail.

■ Use a silent prompt or a voice prompt as a means of foiling hackers and safeguarding your system. A steady tone used as a remote access prompt leaves your system vulnerable to automatic dialing programs.

■ Ring delay can provide added security. Since most automatic dialing programs disconnect if there's no answer after the second or third ring, program your PBX to answer only after the fourth or fifth.

■ Employ call detail recording and examine records regularly to track PBX usage and highlight unusual calling patterns.

■ Make sure your system is physically secure — off-limits to unauthorized personnel. See that all programming-related information is stored under lock and key.

■ Perhaps most important, *educate all employees* on the threat of toll fraud and the steps they can take to prevent it.

[redacted]

Voice mail fraud is growing fast — even faster, say the experts, than PBX-based toll abuse. The reason: voice mail systems provide hackers with the kind of safe haven they enjoyed before the authorities began penetrating underground computer bulletin boards.

To most of us, a voice mail system is a convenient way to leave and retrieve telephone messages. To a toll abuser, it's a trading post for stolen calling cards, PBX access codes, credit card numbers, computer passwords and all manner of other contraband information.

Like PBXs, many voice mail systems offer remote access via local circuits or 800 lines. Using password-cracking software, the hacker calls blocks of local or 800 numbers. Once a number "hits," the hacker proceeds to break the Personal Identification Number (PIN) code and take over the mailbox associated with it. By changing the numeric password, the hacker controls access to the box.

News of the available mailbox spreads throughout the hacker underground, and soon it's full of stolen numbers and passwords for trade or sale. Pirated boxes also may be used for other illegal activities, including drug deals, prostitution, bookie operations and industrial espionage.

[redacted]

Voice mail systems that provide out-dial capability offer hackers an added bonanza, because they can be used to place fraudulent long distance telephone calls.

Hackers have been known to set up voice mailboxes to accept collect calls and even to approve third-number long distance calls.

Voice mail fraud can take on frightening overtones when pirated mailboxes are discovered and attempts are made to shut them down. Hackers sometimes enter the system administrator's personal mailbox and insist on being left alone — or even demand that additional mailboxes be allocated for their use. In one famous case, a hacker vowed to take over an entire voice mail system and lock the administrator out if his demands weren't met. He made good on the threat.

Voice mail fraud — safeguards and countermeasures

■ Understand the functions of your voice mail system, and consult your vendor for advice on system weaknesses.

■ Encourage your vendor to perform on site — not remote — system testing and maintenance.

■ Ensure that out-dial or through-dial capabilities residing within your system are deleted or blocked to prevent access to your local and long distance services via voice mail.

■ Assign your voice mail system a different three-digit prefix than that used by your PBX. For example, if all the telephone numbers at your facility begin with 422, equip your voice mail system with a 538 prefix.

■ *Never* publish the remote access telephone number that connects callers with your voice mail system.

■ Do not allow employees to create their own PINs. Assign PINs randomly, using the maximum number of digits your system will accept. Change PINs periodically.

■ Remove all mailboxes that are not assigned to employees, and limit the time mailboxes may go unused — 30 days is best — before being removed from your system.

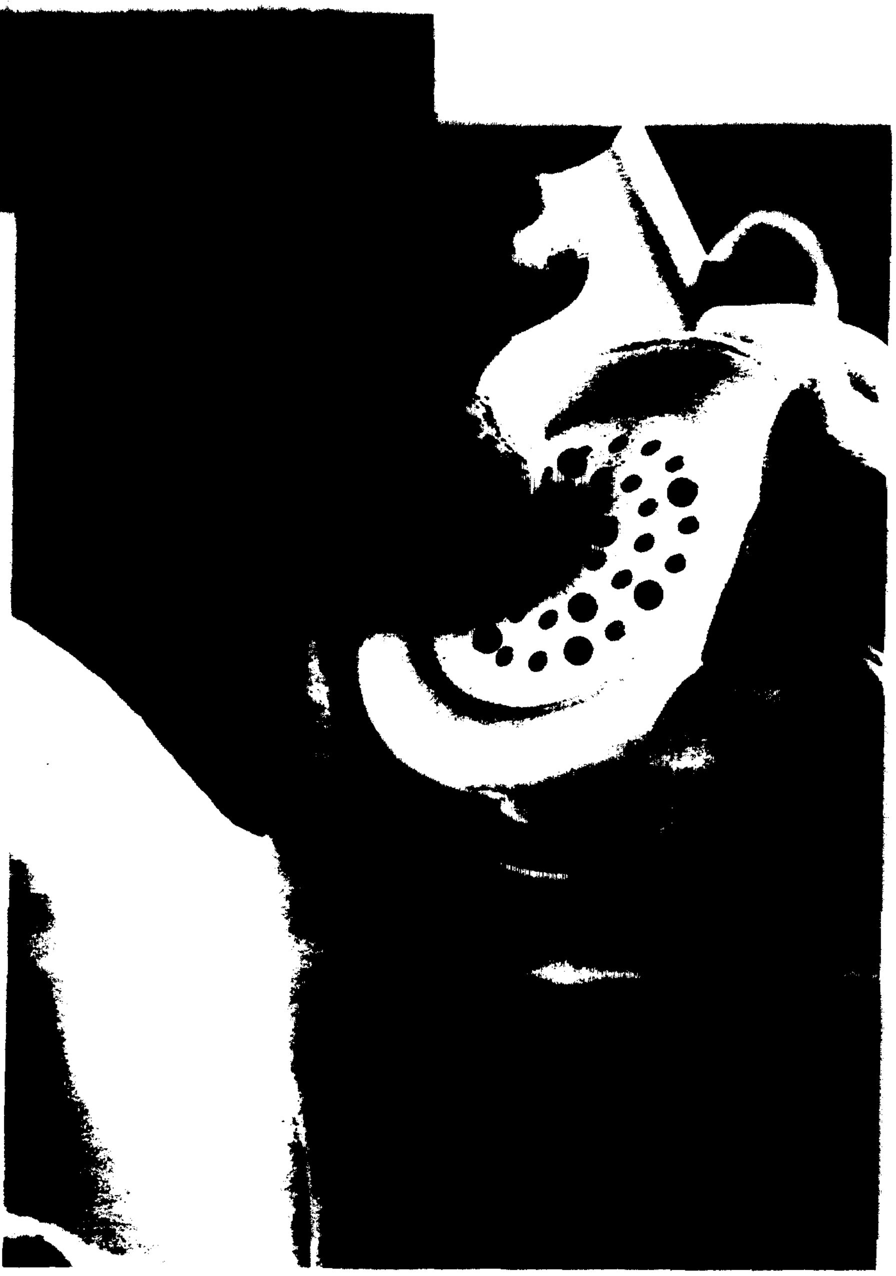
■ Have your system programmed to terminate access after the third invalid attempt to enter a PIN.

■ Limit 800 incoming service only to those areas appropriate to your organization.

■ Use audit trails and examine records on a regular basis to highlight potential voice mail fraud or abuse.

Continued on next page

- Create a proactive plan, not only to prevent voice mail fraud, but to deal with it quickly and effectively in the event that it occurs.
- Make sure PBX console attendants, security officers and remote access users know what to do if they suspect an invasion of your system.
- Promptly deactivate the access codes and voice mail passwords of employees who leave your organization.
- *Educate all employees* on the potential for voice mail fraud and the means of preventing it.



Every new development in telecommunications brings with it a wealth of opportunities — both for honest users and for toll abusers.

Because Electronic Serial Numbers (ESNs) and Mobile Identification Numbers (MINs) are the gateways to cellular service, number-crunching hardware is a key weapon in the cellular hacker's arsenal.

A "chipped up phone," for example, is modified illegally with a microchip that alters the telephone's ESN. A "clone phone" fraudulently duplicates a valid ESN and MIN so that calls placed on it are billed to the legitimate owner. A "tumbler phone" works like a computer hacking program — finding valid ESN's that enable the toll abuser to make untraceable cellular calls — free of charge.

With cellular systems now commonplace, thieves have developed mobile "phone rooms" — vans equipped with cubicles and cellular telephones. Customers converse while the van is driven around the city — a technique that foils efforts to triangulate the location of the operation. Motel rooms also are used for these cellular call-sell operations, most of which deal in international long distance service.

Cellular fraud — safeguards and countermeasures

■ Restrict cellular calling to required areas only. Have your cellular units programmed to disallow international direct dial service.

■ Make sure your cellular users engage the telephone lock feature when their units are not in use.

■ Check cellular bills carefully. At the first indication of misuse, contact your vendor.

■ Because cellular technology is continually changing, consult at least annually with your vendor about the availability of new and more effective security features and devices.

Hacking up close and personal

Ever get the feeling you were being watched?

Not all hacking is done by computer. Sometimes, thieves need to get close to you to obtain the information they seek. You may be observed or overheard while placing a long distance call at an airport, hotel, train station, bus terminal or other public place.

Sharp-eyed hackers scan pay telephone banks and attempt to capture the numbers being entered on touchtone keypads. The technique is known in the trade as "shoulder surfing." Binoculars are a favorite hacker tool for long-range prying. And watch for individuals with camcorders; more and more these days, crooks are stealing codes by making "home movies" of business people dialing their calling card numbers.

Be aware that people who visit your office may not be who they seem to be. Hackers may pose as telephone company personnel, delivery drivers, insurance representatives, lawyers — even FBI agents. In large organizations, they've also been known to impersonate company employees who are lost. "Tailgaters" specialize in entering secure areas directly behind an authorized person.

If allowed free access to your facility, these impostors will seek — and likely find — numeric passwords and other confidential information in offices, on desktops and elsewhere.

Some hackers also are experts at "trashing." They know waste baskets and dumpsters can be gold mines of information. Discarded manuals, company directories, phone books and employee lists can reveal more than you might imagine. Foil the "dumpster divers" with this motto: "Better shred than read."

Person-to-person hacking — safeguards and countermeasures

- When placing calls in public places, be aware of your surroundings. Shield the touchtone keypad with your hand while entering digits. If you are speaking with an operator over a public telephone, watch for potential eavesdroppers and speak in a quiet tone of voice.

- Vendors, repair personnel, delivery drivers and others visiting your office should be able to supply proper identification. To be certain, don't hesitate to call the organization the person claims to represent to confirm his or her identity.

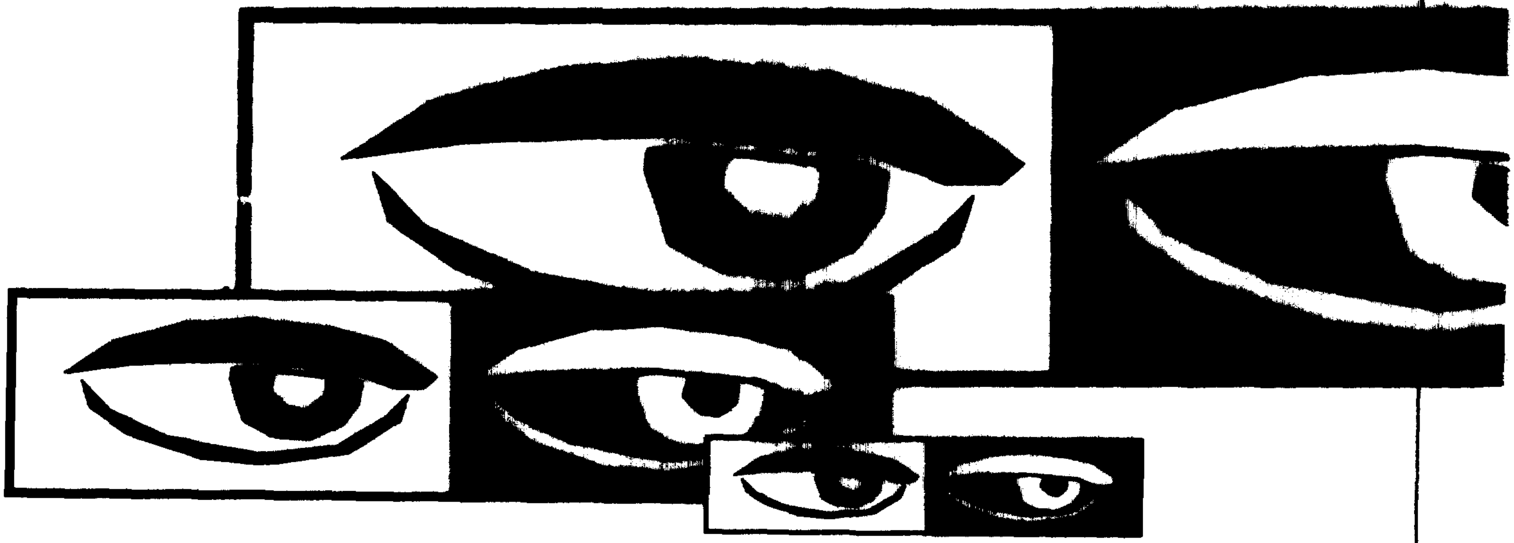
- *Never* reveal access codes or other confidential information without the knowledge and express permission of the appropriate supervisor.

- *Never* leave access codes or similar confidential material on sticky notes or scratch pads near your telephone — or anywhere on your desktop.

- Escort "lost strangers" — especially those without proper identification — to the nearest security desk for assistance.

- Unknown callers requesting information or asking to be transferred within the organization should be treated with respect but handled with care. *Never* reveal confidential information over the telephone. It's always wise to take the caller's name and number and call back. Calls that arouse the slightest suspicion on your part should be referred to security or to the appropriate supervisor.

- Material being discarded should be shredded whenever possible.



Let's work together to fight toll fraud

U S WEST is proud to be a world leader in the telecommunications business. We are committed to resisting the efforts of unscrupulous persons bent on misusing our technologies for criminal purposes.

We hope the information in this brochure will prove helpful to you, and we encourage you to contact your U S WEST representative for counsel and assistance with your toll fraud concerns.

Join us. Together, let's work to keep your systems secure and to reclaim our telecommunications infrastructure from those who would abuse and misuse it!

For additional assistance, you may wish to consult the ***Communications Fraud Control Association,*** *a not-for-profit organization that offers information on toll-fraud-related topics.*
Contact:
The Communications Fraud Control Association
1990 M Street N.W., Suite 508
Washington, D.C. 20036
(202)296-3225

USWEST®
COMMUNICATIONS
Making the most of your time.®